УДК 004.056

Вуз как объект критической информационной инфраструктуры

А. Ю. Солдатов[1], Е. Ю. Солдатов[1], В. С. Скориков[1], Д. Н. Титов[1]*

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация

* e-mail: dglasmann@mail.ru

Аннотация. В статье показана актуальность вопросов, связанных с безопасностью критической информационной инфраструктуры и приведены ключевые понятия, относящиеся к этой сфере защиты информации. Поднимается вопрос безопасности объектов КИИ в высших учебных заведениях; рассматриваются способы и меры защиты сети университета от злоумышленников. В современное время образовательный сектор стал легкой мишенью для всех недоброжелателей. Несмотря на то, что большинство образовательных учреждений России работают в обычном режиме, они продолжают активно использовать цифровые платформы в рамках учебного процесса. Данная тема является актуальной – ведь информационная безопасность высших учебных заведений призвана в первую очередь обеспечить сохранность обрабатываемых персональных данных работников, студентов и абитуриентов. В качестве рекомендации для решения рассмотренных проблем безопасности рекомендован ряд мер, в том числе способ организации защиты локальной сети университета.

Ключевые слова: информационная безопасность, высшее учебное заведение, критическая информационная инфраструктура

University as an object of critical information infrastructure

A. Yu. Soldatov[1], E. Yu. Soldatov[1], V. S. Skorikov[1], D. N. Titov[1]*

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation

* e-mail: dglasmann@mail.ru

Abstract. The article shows the relevance of issues related to the security of critical information infrastructure and provides key concepts related to this area of information protection. The issue of security of CII objects in higher educational institutions is raised; ways and measures to protect the university network from intruders are considered. In modern times, the educational sector has become an easy target for all ill-wishers. Despite the fact that most educational institutions in Russia operate as usual, they continue to actively use digital platforms as part of the educational process. This topic is relevant - after all, the information security of higher educational institutions is designed primarily to ensure the safety of the processed personal data of employees, students and applicants. As a recommendation for solving the considered security problems, a number of measures are recommended, including a method for organizing the protection of the university's local network.

Keywords: information security, higher educational institution, critical information infrastructure

Введение

2021 год стал рекордным по количеству утечек данных банков, социальных сетей, веб-сервисов, мобильных приложений. Согласно исследованию Identity Theft Resource Center (ITRC), общее количество утечек данных до 30 сентября 2021 года уже превысило общее количество событий в 2020 году на 17 %: 1291 утечка данных в 2021 году по сравнению с 1108 утечками в 2020 году.

Технологии, компьютеры и ИКТ уже быстро становятся неотъемлемой частью работы и ведения бизнеса многих из нас. Интернет произвел революцию в общении, и теперь это наше предпочтительное средство повседневного общения. Почти во всем, что мы делаем, мы используем Интернет. Заказ пиццы, покупка телевизора, общение с другом, отправка изображения через мгновенные сообщения. До Интернета, если мы хотели быть в курсе новостей, нам приходилось идти к газетному киоску и покупать местное издание, сообщающее о том, что произошло накануне. Но сегодня достаточно одного или двух кликов, чтобы прочитать местную газету и любой источник новостей из любой точки мира, обновляемый с точностью до минуты.

Цели кибератак обширны: они совершаются не только на органы власти и бизнес, в их прицел попадают и система образования, и вузы. Чаще всего кибератакам подвергаются объекты критической информационной инфраструктуры (КИИ): информационные системы, информационно-телекоммуникационные системы, автоматизированные системы управления государственных учреждений и компаний, которые функционируют во всех областях жизнеобеспечения городов, субъектов всей страны, что доказывают события последних лет [1].

К примеру, абитуриенты колледжей Гриннелл, Гамильтон и Оберлин получили записки с требованием выкупа от хакеров, утверждающих, что они получили доступ к файлам их приложений. Три элитных колледжа используют общую систему данных под названием Slate, которая отслеживает прием абитуриентов. Сообщается, что украденные данные включали личную информацию, а также конфиденциальную, заметки сотрудников приемной комиссии, отчет об их собеседовании и решения о приеме.

Образовательный сектор стал легкой мишенью для злоумышленников, поскольку он не уделяет первостепенное внимание кибербезопасности, в то время как пандемия «вынудила преподавателей стать случайными ИТ-директорами», поскольку они стремились перевести сотрудников и студентов на новые online технологии.

Методы и материалы

В принятом 8 февраля 2018 г. постановлении Правительства №127 «Об утверждении показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, а также порядка и сроков осуществления их категорирования» определены характеристики критериев значимости, порядок и сроки категорирования объектов КИИ.

Главными органами, которые осуществляют функции регулирования и контроля за исполнением этого общегосударственного закона, являются ФСТЭК и ФСБ [2].

Одним из самых главных составляющих 187-ФЗ является категорирование. Категорирование позволяет правильно расставить приоритеты субъекта и сформировать систему защиты.

Одна из первых задач субъектов КИИ – определение перечня объектов и, соответственно, их категорирование. Как видно из практики, почти все субъекты

с этим не управляются. Рассмотрим сферу науки, а конкретно высшие образовательные учреждения (университет).

Большое количество высших учебных заведений могут относиться к субъектам критической информационной инфраструктуры, так как кроме образовательной деятельности, они проводят финансируемые и инициативные научные исследования. Для этого используется различное научное программное обеспечение, например, «Mathcad» и «AnyLogic», которое может моделировать системы любой сложности. Также в структуре университетов могут находиться структурные подразделения, которые имеют возможность заниматься научной деятельностью [3].

Можно сделать вывод, что большая часть высших учебных заведений является субъектами критической информационной инфраструктуры, и попадает под действие законодательства о безопасности КИИ. Соответственно, эти информационные системы нужно защищать [4].

У правонарушителя могут быть разные мотивы вторжения в сеть университета. К примеру, у него есть цель скомпрометировать научные разработки и исследования. Еще одной причиной вторжения может быть остановка образовательного процесса путем частичного/полного разрушения электронной информационно-образовательной среды вуза.

Результаты

Для решения данной проблемы нами был предложен способ организации защиты локальной сети университета с использованием таких СЗИ, как ViP Net Coordinator, IDSNS, TIAS и xFirewall (рис. 1) [5].

Самые уязвимые узлы сети – это сервер базы данных и файловый сервер, т. к. на этом участке сети отсутствует xFire Wall.

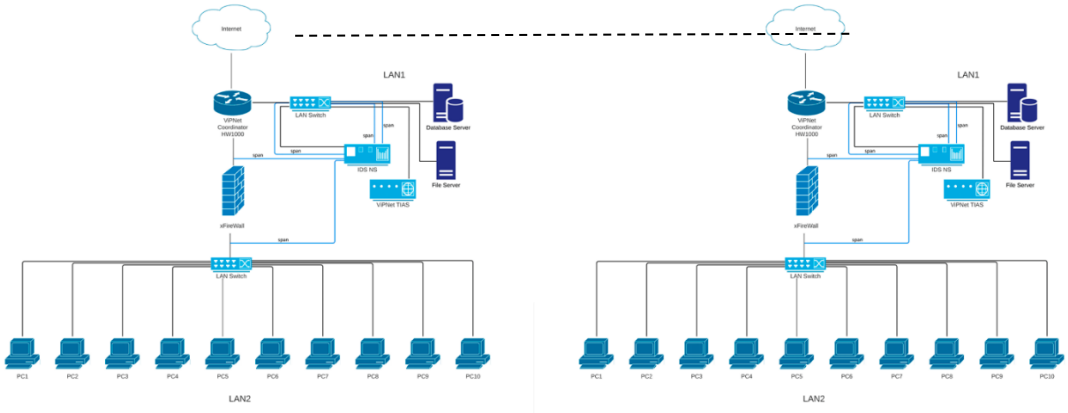

Рис. 1. Схема защиты локальной сети вуза

Для защиты отдельных хостов на каждом узле LAN2 установлена ViP Net Safe Boot, ViPNet SafePoint и Endpoint Protection Platform (EPP).

PC10 отведен под администрирование: на узле установлен ViPNet Client, ViPNet Administrator, ViPNet MC для ПАК ViPNet TIAS.

Опираясь на 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017, владельцы объектов критической информационной инфраструктуры должны подключиться к ГосСОПКА.

Обсуждение

Вторжение в сеть извне, что представлено на рисунке 1, будет сильно затруднено благодаря внедрению указанных выше СЗИ. Попыткам вторжения внутрь сети препятствуют IDS NS и xFireWall. Применение ПАК TIAS помогает выявлять инциденты на основе анализа событий информационной безопасности.

Заключение

Таким образом, соблюдение требований в области безопасности КИИ для вузов имеет решающее значение. Идеальной системы не существует, пока в этой системе находится человек. Нами был изучен вопрос, как усовершенствовать системы защиты в технической области. Включение в сеть различных СЗИ (например, решения компании ИнфоТеКС) является одним из оптимальных решений по защите инфраструктуры вуза.

Нынешняя ситуация в мире даёт ясное видение того, как использование различных методов вторжения может нанести ущерб организациям, в том числе образовательным учреждениям с последующей остановкой образовательного процесса.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Информационная безопасность высших учебных заведений. – Текст: электронный // ИТ-Энигма: официальный сайт – 2021. – URL: https://it-enigma.ru/resheniya/vuzi/ – (дата обращения: 03.05.2022).

2. Постановление Правительства Российской Федерации от 8 февраля 2018 г. N 127 // ФСТЭК России: официальный сайт – 2018. – URL: https://vk.cc/cd8TP5 – (дата обращения: 03.05.2022).

3. Категорирование объектов критической информационной инфраструктуры // Фундаментальные и прикладные научные исследования: официальный сайт – 2019. – URL: https://naukaip.ru/wp-content/uploads/2019/06/MK-572-2.pdf – (дата обращения: 03.05.2022).

4. Категорирование объектов критической информационной инфраструктуры (КИИ) // RTMGroup: официальный сайт – 2018. – URL: https://vk.cc/cd8Y9H – (дата обращения: 03.05.2022).

5. Продукты компании Инфотэкс// Infotecs: официальный сайт – 2022. – URL:https://infotecs.ru/product/setevye-komponenty/ – (дата обращения: 03.05.2022).